

1 **CLAIMS**

2
3 1. A processor-readable medium comprising processor-executable
4 instructions configured for:

5 receiving a binary signature;
6 receiving a security patch;
7 identifying a vulnerable binary file on a computer based on the binary
8 signature; and
9 updating the vulnerable binary file on the computer with the security patch.
10

11 2. A processor-readable medium as recited in claim 1, wherein the
12 identifying a vulnerable binary file on a computer includes comparing a bit pattern
13 of the binary signature against binary files located on the computer, the bit pattern
14 associated with a security vulnerability.
15

16 3. A processor-readable medium as recited in claim 1, wherein the
17 updating the vulnerable binary file on the computer includes installing the security
18 patch on the computer.
19

20 4. A processor-readable medium as recited in claim 1, wherein the
21 identifying a vulnerable binary file on a computer includes sending the binary
22 signature to the computer.
23

24 5. A processor-readable medium as recited in claim 4, wherein the
25 updating the vulnerable binary file on the computer includes:

1 receiving a request from the computer to send the security patch; and
2 sending the security patch to the computer.

3
4 6. A processor-readable medium as recited in claim 1, wherein the
5 computer is a client computer and the receiving includes receiving the binary
6 signature and the security patch from a distribution server configured to distribute
7 to the client computer, binary signatures that identify vulnerable files and security
8 patches configured to fix the vulnerable files.

9
10 7. A server comprising the processor-readable medium as recited in
11 claim 1.

12
13 8. A processor-readable medium comprising processor-executable
14 instructions configured for:

15 receiving a binary signature that identifies a security vulnerability in a
16 binary file;

17 receiving a security patch configured to fix the security vulnerability in the
18 binary file; and

19 distributing the binary signature and the security patch to a plurality of
20 servers.

21
22 9. A processor-readable medium as recited in claim 8, wherein the
23 distributing includes:

24 sending a notice to each of the plurality of servers regarding the security
25 vulnerability and the available patch;

1 receiving a request to send the binary signature and the security patch; and
2 sending the binary signature and the security patch in response to the
3 request.

4
5 **10.** A distribution server comprising the processor-readable medium as
6 recited in claim 8.

7
8 **11.** A processor-readable medium comprising processor-executable
9 instructions configured for:

10 receiving a binary signature from a server;
11 searching for the binary signature in binary files;
12 sending a request to the server for a security patch if a binary file is found
13 that includes the binary signature;
14 receiving the security patch from the server; and
15 updating the binary file with the security patch.

16
17 **12.** A client computer comprising the processor-readable medium as
18 recited in claim 11.

19
20 **13.** A method comprising:

21 receiving a binary signature;
22 searching for a vulnerable file based on the binary signature;
23 if a vulnerable file is found, requesting a security patch; and
24 fixing the vulnerable file with the security patch.
25

1 **14.** A method as recited in claim 13, wherein the requesting includes
2 sending a request to a server for the security patch, the method further comprising
3 receiving the security patch from the server in response to the request.

4
5 **15.** A method as recited in claim 14, wherein the receiving includes
6 receiving the binary signature from the server.

7
8 **16.** A method as recited in claim 13, wherein the fixing includes
9 installing the security patch on a computer.

10
11 **17.** A method as recited in claim 13, wherein the searching includes
12 comparing the binary signature to binary information on a storage medium of a
13 computer.

14
15 **18.** A method as recited in claim 17, wherein the binary information is
16 selected from the group comprising:

17 an operating system;
18 an application program file; and
19 a data file.

20
21 **19.** A method as recited in claim 17, wherein the storage medium is
22 selected from the group comprising:

23 a hard disk;
24 a magnetic floppy disk;
25 an optical disk;

1 a flash memory card;
2 an electrically erasable programmable read-only memory; and
3 network-attached storage.
4

5 **20.** A method comprising:
6 receiving a binary signature and a security patch from a distribution server;
7 searching on a client computer for a vulnerable file associated with the
8 binary signature; and
9 if a vulnerable file is found, fixing the vulnerable file with the security
10 patch.
11

12 **21.** A method as recited in claim 20, wherein the searching includes
13 transferring the binary signature to the client computer, the client computer
14 configured to search for a vulnerable file associated with the binary signature.
15

16 **22.** A method as recited in claim 21, wherein the fixing includes:
17 receiving a request from the client computer to transfer the security patch,
18 the client computer having located a vulnerable file; and
19 transferring the security patch to the client computer in response to the
20 request.
21

22 **23.** A computer comprising:
23 means for receiving a binary signature;
24 means for searching for a vulnerable file based on the binary signature;
25 means for requesting a security patch if a vulnerable file is found; and

1 means for fixing the vulnerable file with the security patch.

2
3 **24.** A server comprising:

4 means for receiving a binary signature and a security patch from a
5 distribution server;

6 means for scanning a client computer for a vulnerable file associated with
7 the binary signature; and

8 means for fixing the vulnerable file with the security patch if a vulnerable
9 file is found.

10
11 **25.** A computer comprising:

12 binary information;

13 a scan module configured to receive a binary signature and scan the binary
14 information for the binary signature; and

15 a patch module configured to request a security patch and install the
16 security patch if the binary signature is found in the binary information.

17
18 **26.** A computer as recited in claim 25, further comprising a storage
19 medium configured to retain the binary information.

20
21 **27.** A computer as recited in claim 25, wherein the binary information is
22 selected from the group comprising:

23 an operating system;

24 an application program file; and

25 a data file.

1
2 **28.** A computer comprising:
3 binary files;
4 a binary signature; and
5 a security patch module configured to receive the binary signature from a
6 server and to scan the binary files in search of the binary signature.

7
8 **29.** A computer as recited in claim 28, further comprising:
9 a binary file that includes the binary signature; and
10 a security patch;
11 wherein the security patch module is further configured to request the
12 security patch from the server upon locating the binary signature within the binary
13 file, and to apply the security patch to the binary file.

14
15 **30.** A distribution server comprising:
16 a database; and
17 a distribution module configured to receive a binary signature and a security
18 patch, store the binary signature and the security patch in the database, and
19 distribute the binary signature and the security patch to a plurality of servers.

20
21 **31.** A distribution server as recited in claim 30, wherein the distribution
22 module is further configured to receive a request from a server for the binary
23 signature and the security patch and to distribute the binary signature and the
24 security patch to the server in response to the request.
25

1
2 **32.** A server comprising:
3 a binary signature associated with a security vulnerability in a binary file;
4 a security patch configured to fix the security vulnerability in the binary
5 file; and
6 a scan module configured to scan binary files on a client computer for the
7 binary signature and to update the binary file with the security patch if the binary
8 signature is found.

9
10 **33.** A server as recited in claim 32, further comprising:
11 a database;
12 the scan module further configured to receive the binary signature and the
13 security patch from a distribution server and to store the binary signature and the
14 security patch in the database.